

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION  
(PCT Rule 61.2)

Date of mailing:

01 February 2001 (01.02.01)

To:

Commissioner  
US Department of Commerce  
United States Patent and Trademark  
Office, PCT  
2011 South Clark Place Room  
CP2/5C24  
Arlington, VA 22202  
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

International application No.:

PCT/GB00/02813

Applicant's or agent's file reference:

A25806 WO

International filing date:

20 July 2000 (20.07.00)

Priority date:

23 July 1999 (23.07.99)

Applicant:

BRISCOE, Robert, John

1. The designated Office is hereby notified of its election made:



in the demand filed with the International preliminary Examining Authority on:

30 October 2000 (30.10.00)



in a notice effecting later election filed with the International Bureau on:

2. The election  was

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO

34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

## PATENT COOPERATION TREATY

## PCT

REC'D 07 DEC 2001
WIPO
PCT

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

14

Applicant's or agent's file reference <b>A25806 WO</b>	<b>FOR FURTHER ACTION</b>	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. <b>PCT/GB00/02813</b>	International filing date (day/month/year) <b>20/07/2000</b>	Priority date (day/month/year) <b>23/07/1999</b>

International Patent Classification (IPC) or national classification and IPC  
**H04L9/08**Applicant  
**BRITISH TELECOMMUNICATIONS publ.ltd.co.**

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 9 sheets, including this cover sheet.
  - This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 1 sheets.

3. This report contains indications relating to the following items:

- I  Basis of the report
- II  Priority
- III  Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV  Lack of unity of invention
- V  Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI  Certain documents cited
- VII  Certain defects in the international application
- VIII  Certain observations on the international application

Date of submission of the demand <b>30/10/2000</b>	Date of completion of this report <b>05.12.2001</b>
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer  Apostolescu, R  Telefono No. +49 89 2399 7950



INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT

International application No. PCT/GB00/02813

**I. Basis of the report**

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17)*):  
**Description, pages:**

1-42 as originally filed

**Claims, No.:**

1-19,23,24 as originally filed

20-22,25 as received on 26/10/2001 with letter of 23/10/2001

**Drawings, sheets:**

1/19-19/19 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- the language of publication of the international application (under Rule 48.3(b)).
- the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- contained in the international application in written form.
- filed together with the international application in computer readable form.
- furnished subsequently to this Authority in written form.
- furnished subsequently to this Authority in computer readable form.
- The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. PCT/GB00/02813

- the description,      pages:  
 the claims,      Nos.:  
 the drawings,      sheets:
5.  This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).  
*(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)*
6. Additional observations, if necessary:

**III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability**

1. The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:
- the entire international application.  
 claims Nos. 20-25.
- because:
- the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):
- the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 20-25 are so unclear that no meaningful opinion could be formed (*specify*):  
**see separate sheet**
- the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.
- no international search report has been established for the said claims Nos. .
2. A meaningful international preliminary examination cannot be carried out due to the failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions:
- the written form has not been furnished or does not comply with the standard.  
 the computer readable form has not been furnished or does not comply with the standard.

**V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. PCT/GB00/02813

**1. Statement**

Novelty (N)	Yes:      Claims 1-10, 12-19
	No:      Claims 11
Inventive step (IS)	Yes:      Claims 1-10, 12-19
	No:      Claims 11
Industrial applicability (IA)	Yes:      Claims 1-19
	No:      Claims

**2. Citations and explanations  
see separate sheet**

**VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:  
**see separate sheet**

**VIII. Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

**see separate sheet**

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/GB00/02813

**Re Item III**

**Non-establishment of opinion with regard to novelty, inventive step and industrial applicability**

See Re Item VIII.

**Re Item V**

**Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

Reference is made to the following documents:

- D1: DE 195 11 298 A (DEUTSCHE TELEKOM AG) 2 October 1996 (1996-10-02)
- D2: WO 99 33242 A (BRISCOE ROBERT JOHN ;FAIRMAN IAN RALPH (GB); BRITISH TELECOMM (GB)) 1 July 1999 (1999-07-01) cited in the application
- D3: EP-A-0 800 293 (LUCENT TECHNOLOGIES INC) 8 October 1997 (1997-10-08)
- D4: McGREW and SHERMAN: 'Key Establishment in Large Dynamic Groups Using One-Way Function Trees', May 20, 1998, p.1-13 Available from Internet: <URL:<http://www.cs.umbc.edu/~sherman>> 20 December 1999  
XP002126220

**1. Independent claims 1, 12, 18 and 19.**

It is considered that independent claims 1, 12, 18 and 19 relate to new and inventive subject-matter (Articles 33 (2) and (3) PCT), since the prior art does not disclose or suggest the specifically claimed method of distributing data according to claim 1, does not disclose or suggest the specifically claimed method of communicating data to a group of users according to claim 12, does not disclose or suggest the specifically claimed method features according to claim 18 and does not disclose or suggest the specifically claimed method of operating a user terminal according to claim 19.

Document D2 describes a method of distributing encoded data to a multiplicity of users. A seed value for key generation is communicated to said users and the encoded data is decoded using keys derived from said seed value.

Document D4 is directed to key establishment in large dynamic groups using one-way function trees.

Claim 1 of the present invention discloses a method of distributing data characterized in that a double bound portion of a sequence of keys is generated at an user terminal and the position of the lower and upper bounds of the portion in the sequence are determined by the at least one seed value communicated to said user terminal.

Claim 12 of the present invention discloses a method of communicating encrypted data to a group of users characterised in that a number of intermediate seed values are generated at the user terminal from a number of initial seed values and in that a plurality of keys used in encrypting the data are derived from said intermediate seed values.

Claim 18 of the present invention discloses a method of distributing encrypted data units characterized in that the encryption keys are held by a third party key manager such that in use receivers may obtain keys for access to an arbitrary portion of the data from the key manager without reference to any data sender or senders.

Claim 19 of the present invention discloses a method of operating a user terminal characterised in that an arbitrarily doubly bounded key sequence is generated at the user terminal from one or more received seed values and in that the received encrypted data units are decrypted using values of said generated key sequence.

**2. Dependent claims 2 to 10 and 13 to 17.**

Dependent claims 2 to 10 and 13 to 17 contain further details of the method claims 1 and respectively 12. As they are dependent on claims 1 and respectively 12 they also satisfy the requirements for novelty and inventive step (Article 33 (2) and (3) PCT).

**3. Independent claim 11.**

Document D4 (see in particular sections 1, 4, 4.1, 4.2 and 7), which is considered to represent the most relevant state of the art, discloses, according to all features of claim 11, a method of encrypting data for distribution comprising:

- ◆ operating on at least one root seed value with one or more blinding functions, thereby producing a plurality of further values (section 4.1, Property 3);
- ◆ operating with one or more blinding functions on the further values produced by the preceding step or on values derived therefrom (section 4.1, Property 3);
- ◆ iterating step (b) and thereby producing, by the or each iteration, a next successive layer in a tree of values (section 4.1, section 4.2);
  
- ◆ encrypting a plurality of data units using a sequence of key values derived from one or more of the layers generated by step (c) (section 1, section 4, section 4.1, section 4.2 and section 7).

All the features described in claim 11 are thus known from document D4.

The subject-matter of claim 11 is therefore not new (Article 33 (2) PCT).

Furthermore, even if the applicant were to interpret claim 11 in such a manner as to enable it to allege that its subject-matter is novel, nevertheless the subject-matter does not seem to involve an inventive step (Article 33 (3) PCT) in the light of document D4.

Same outcome, i. e. independent claim 11 does not meet the requirements of the PCT in respect of inventive step, is to be expected when the person skilled in the art would combine his general knowledge about iterated hash functions (for example the iterated one-way-hash-function OWHF) with the disclosure of D4.

**Re Item VII**

**Certain defects in the international application**

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in the documents D1 to D4 is not mentioned in the description, nor are these documents identified therein.

2. Independent claims 11, 19, 20, 21, 22 and 25 are not in the two-part form in accordance with Rule 6.3(b) PCT.

3. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).

4. The statements of the description as for example:

- ◆ " ... will be presented in Section 4.5, ..." (page 13, line 16)
- ◆ " ... the BHC-T hybrid in Fig 4.3.2." (page 25, line 26)
- ◆ " ... amortised initialisator [Balen99]." (page 34, line 30)

are inconsistent.

**Re Item VIII**

**Certain observations on the international application**

1. Although claims 1, 12 and 19 have been drafted as separate independent method claims, they appear to relate effectively to the same subject-matter and to differ from each other only with regard to the definition of the subject-matter for which protection is sought or in respect of the terminology used for the features of that subject-matter. The aforementioned claims therefore lack conciseness.

Moreover, lack of clarity of the claims as a whole arises, since the plurality of independent claims makes it difficult, if not impossible, to determine the matter for which protection is sought, and places an undue burden on others seeking to establish the extent of the protection.

Although claims 21, 22 and 25 have been drafted as separate independent apparatus claims, they appear to relate effectively to the same subject-matter and to differ from

each other only with regard to the definition of the subject-matter for which protection is sought or in respect of the terminology used for the features of that subject-matter. The aforementioned claims therefore lack conciseness.

Moreover, lack of clarity of the claims as a whole arises, since the plurality of independent claims makes it difficult, if not impossible, to determine the matter for which protection is sought, and places an undue burden on others seeking to establish the extent of the protection.

Hence, claims 1, 12 and 19 and respectively 21, 22 and 25 do not meet the requirements of Article 6 PCT.

2. Claims 20, 21, 22 and 25 are not acceptable in their present form because they do not meet the requirements following from Article 6 PCT taken in combination with Rule 6.3 PCT that any independent claim must contain all technical features essential to the invention.

A claim for an apparatus should not seek to define the invention by referring to features which concern the effect which is desired to achieve (Guidelines C-III, 4.7). Formulation like "...arranged to operate..." or "... for use in a..." are in this case not sufficient to clearly define the invention and it is rather constructional details of the various apparatus which should have appeared in the claims.